REMARKS

Claim Objections

The examiner "objected to" Claims 4, 17, 27, and 31. As a threshold, Applicant considers this objection to in fact be a rejection of the cited claims under 35 U.S.C. 112, second paragraph, reviewable by the Board of Patent Appeals and Interferences.

The examiner stated:

> **Claims 4, 17, 27, and 31 are objected to as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 4, 17, 27, and 31 recite "more than 'C3' new host pairs," the type of variable "C3" is undefined. The examiner respectfully points to independent claim 1 as an example for defining the type of variables being claimed, independent claim 1 defines variable "C1" as a first threshold number and "C2" as a first factor value.**

Claims 4, 17, 27 and 31 are indeed defined by Applicant's claims and specification. For instance the variable C3 is indeed as the examiner recognizes a variable. The type of variable is "new host pairs over the second update period." One of ordinary skill in this art would clearly appreciate that C3 is part of an equation and that C3 is a measurement of the number of new host pairs found in the connection table from a second update period table, having a period that is greater in duration than the first update period (of claim 1) in order to check for ping scans at the end of the second update period.

The examiner also stated:

> **2. Claim 5 is objected to because of the following informalities: claim 5 recites "a first threshold number 'C4'," on line 8 and "a first factor value 'C5'," on line 10 it is unclear whether the recited claim limitations are intended to refer to "a first threshold number 'CI'," and "first factor value 'C2'," recited in independent claim 1.**
>
> **3. Claim 18 is objected to because of the following informalities: claim 18 recites "a first threshold number 'C4'," on line 19 and "a first factor value 'C5'," on line 20 it is unclear whether the recited claim limitations are intended to refer to "a first threshold number 'C1'," and "first factor value 'C2'," recited in independent claim 14.**
>
> **4. Claim 32 is objected to because of the following informalities: claim 32 recites "a first threshold number 'C4'," on line 18 and "a first factor value 'C5'," on line 19 it is unclear whether the recited claim limitations are intended to refer to "a**

> **first threshold number 'C1'," and "first factor value 'C2'," recited in independent claim 28.**

Claims 5, 18 and 32 are defined by Applicant's claims and specification. For instance the variable C4 and C5 are relevant to the second update period and define a first threshold number "C4" host pairs and a first factor C5 pertaining to the second update period.

Allowable Subject Matter

At the outset Applicant thanks the examiner for indicating that Claims 5, 18, 32 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

For reasons discussed below Applicant believes that all of the claims are allowable.

35 U.S.C. 102

The examiner rejected Claims 1-4, 6-17, 19-31, and 33-36 under 35 U.S.C. 102(e) as being anticipated by Pruthi (US 20041001 5581).

Regarding Claims 1, 14, 24, and 28, the examiner stated:

> **Pruthi discloses a method of detecting scanning attacks that adds host-pair connection records to a connection table ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) stored on a computer readable ("Short-term Memory" and "Long-term Memory" See fig. 5 ref. nos. 508 and 51 0) medium when a host accesses another host, at the end of a first update period accessing the connection table to determine new host pair ("The start field specifies the beginning time from which the traffic is analyzed and its results are displayed on the GUI." and "The stop field specifies the ending time to which the traffic is analyzed and its results are displayed on the GUI." See paragraphs 92-93), determining the number of new host pairs added to the connection table over the first update period ("The number of IP host pair connections involving a common IP address exceeds x over a time window y." See paragraph 187), and if a host has made more than a first threshold number "CI" host pairs ("Threshold x" See paragraph 187) and an historical number of host pairs is smaller than the threshold number by a first factor value "C2" ("The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network." See paragraph 200) then indicating that the new host is a scanner ("Providing a request for action in response to a pattern indicative of an intruder" See paragraphs 172-1 87).**

In addressing Applicant's prior reply the examiner added the following:

> **In response to the applicants' argument that Pruthi does not disclose "adding host-pair connection records to a connection table," and therefore Pruthi does not "determine the number of new host pairs added to the table over the first update period." The examiner respectfully points the applicants to Host-Pairs Table shown in figure 14 ref. no. 1402 and paragraphs 115-116. The examiner further points the applicants to the updating to the Host-Pairs Table over an operator specified time period disclosed in paragraphs 92-93.**
>
> **In response to applicants' argument that Pruthi does not disclose "a first update period," "a first threshold number 'CI'," and "a first factor value 'C2'," the examiner respectfully points out that Pruthi discloses a time window y in paragraphs 92-93 and 187 that corresponds to "a first update period," a threshold x in paragraph 187 that corresponds to "a first threshold 'CI'," and inherently discloses a historical number of host pairs created by normal operating traffic over the network in paragraph 200 with the difference between the threshold x and the historical number corresponds to "a first factor value 'C2'." The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, through selecting a value for threshold x that is greater than the historical number of host pair connections made by normal operating traffic over the network. This selection allows the for the method of detecting scanning attacks to function properly by alerting the operator when the network is under scanning attacks as opposed to alerting the operator is always under scanning attacks when normal operating traffic is on the network.**
>
> **The examiner further points out that prior art is presumed to operable and enabled. A reference contains and enabling disclosure if the public was in possession of the claimed invention before the date of invention and such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his own knowledge to make the claimed invention. See MPEP 2121.01**

These claims are allowable over Pruthi. Claim 1, for example, requires, "a … method of detecting scanning attacks and includes the features of: "adding host-pair connection records to a connection table stored on a computer readable medium when a host accesses another host; at the end of a first update period, accessing the connection table to determine new host pairs; determining the number of new host pairs added to the connection table over the first update period; and if a host has made more than a first threshold number "C1" host pairs, and an historical number of host pairs is smaller than the threshold number by a first factor value "C2", then indicating that the new host is a scanner."

The examiner argues that the connection table is taught by Pruthi at "**a connection table ("Host-Pairs Table" See fig. 14 ref. no. 1402 and paragraphs 115-116) stored on a computer readable ("Short-term Memory" and 'Long-term Memory'**" Short term and long term memory are described by Pruthi in [0047], reproduced below:

> [0047] The packets may be directly stored into the short-term memory 510 using path A. This is useful for storing all data received from the communication line. The short-term memory 508 may periodically transfer data to a long-term memory 510 to prevent overflow. Although illustrated as having only a single short-term memory 508 and a single long-term memory 510, the teachings of the present invention are applicable to other hierarchical memory structures including a plurality of memory devices. For example, the memory may include a random access memory (RAM), a disk memory, and a tape memory. As the RAM fills, data is transferred to the disk memory. As the disk memory fills, data is transferred to the tape memory. As the tape memory fills, tapes are replaced for continuous or long-term data storage for archival purposes, for example. As indicated by the double arrow to the short-term memory 508 and between the memories 508, 510, data stored in the memories may later be retrieved for analysis or for one of the applications 522-530 discussed below.

Thus rather than possessing the features of the claimed connection table, the short and long term memories are merely different hierarchical layers of plain vanilla storage, possessing none of the features of the claimed connection table. As for paragraphs 92-93 referred to by the examiner in addressing Applicant's prior reply, these paragraphs describe start and stop times for analysis, but again none of the features of the claimed connection table.

The examiner also relies on Pruthi to describe **determining the number of new host pairs added to the table over the first update period (0187).**" However, as pointed out above Pruthi neither describes nor suggests "new host pairs" added to a table over an update period whether at [0187] or elsewhere.

Pruthi does mention scans. However, Pruthi does not detect scans in the manner called for by claim 1. The examiner relies on [0187] for the features of Applicant's claim pertaining to and if a host has made more than a first threshold number "CI" host pairs. Pruthi describes in [0187]:

> **[0187] For a particular set of applications, the number of IP host pair connections involving a common IP address (either the source or destination) exceeds x over a time window of y. x and y should be user configurable. The set of applications should include a set of positive rules, e.g. telnets and pings, as well as negative rules such as "not http". This can be used to track Denial of Service attacks and IP host scans.**

Claim 1 requires: "determining the number of new host pairs added to the table over the first update period." Applicant contends that not only does Pruthi fail to disclose the table; Pruthi fails to determine the number of new host pairs added to the table over the first period. Pruthi merely determines "**the number of IP host pair connections involving a common IP address (either the source or destination) exceeds x over a time window of y.**" This however is neither relevant to nor determines <u>new</u> host pairs.

The claimed feature also requires evaluation of two thresholds i.e., "if a host has made more than ... "C1" host pairs," and requires determining if ... the number C1 is smaller than "an historical number of host pairs" by a first factor value "C2" to indicate that the new host is a scanner. Pruthi has two user configurable variables "**the number of IP host pair connections involving a common IP address**" that exceeds "**x**" and "**y**" a "**time window.**" While Applicant does not concede that "**x**" corresponds to "C1," it is quite clear that Applicant requires three items, "C1," an update period and "C2."

The examiner also argues that: "**("The examiner respectfully points out that it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly, as opposed to alerting the operator that the network is always under scanning attacks when normal operating traffic is on the network." See paragraph 200) then indicating that the new host is a scanner ("Providing a request for action in response to a pattern indicative of an intruder" See paragraphs 172-1 87).**" Applicant disagrees that the historical number of host pairs is inherent in Pruthi.

Rather, Pruthi describes a different technique as set out in 187-191, not 172-187 as the examiner contends. Paragraphs 187-191 are reproduced below:

> **[0187] For a particular set of applications, the number of IP host pair connections involving a common IP address (either the source or destination) exceeds x over a time window of y. x and y should be user configurable. The set of applications should include a set of positive rules, e.g. telnets and pings, as well as negative rules such as "not http". This can be used to track Denial of Service attacks and IP host scans.**
>
> **[0188] For a particular IP host pair, the byte rate exceeds x or over a sustained period of y. x and y should be user configurable. The set of applications should include a set of positive rules, e.g. telnets and pings, as well as negative rules such as "not http".**
>
> **[0189] This can be used to track suspicious "excessive" usage to a destination from a particular source. For example, break-ins to a particular host.**
>
> **[0190] For a particular IP host, the number of individual sessions exceeds x or over a sustained period of y. x and y should be user configurable. The set of**

> **applications should include a set of positive rules, e.g. telnets and pings, as well as negative rules such as "not http".**
>
> **[0191] This can be used to track suspicious "excessive" session activities to a destination from a particular source. For example, break-ins to a particular host.**

"Host pair connections" is mentioned twice in Pruthi, so it is inconceivable that Pruthi describes the claimed connection table. Secondly, as Pruthi describes, Pruthi looks for an number of source-destination addresses that exceed a threshold over a time window. Pruthi looks for byte rates that exceed a threshold over a period and excessive session activities. However, nothing is mentioned of historical comparisons.

Moreover, the examiner appears to improper attack the efficacy of the teachings in the reference. If the examiner contends that "**it is inherent that the operator has access to the historical number of host pairs created by normal operating traffic over the network. The historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly**" then what the examiner is saying is that Pruthi has an non-enabling disclosure because Pruthi failed to describe some feature that according to this examiner is at the core of the process to detect scan attacks (**historical number is necessary for the method of detecting scanning attacks disclosed by Pruthi to function properly**). This would appear to be administratively improper for the examiner to argue.

Accordingly at least for these reasons Pruthi neither describes nor suggests claim 1.

Applicant's dependent Claims add additional patentably distinct features for the reasons of record.

This Reply is accompanied by a Notice of Appeal.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

The Extension of Time fee of **$65** is being paid concurrently on the electronic filing system by way of Deposit Account authorization. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: February 20, 2009

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945